



UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

| APPLICATION NO. | FILING DATE | FIRST NAMED INVENTOR | ATTORNEY DOCKET NO. | CONFIRMATION NO. |
|--|-------------|----------------------|---------------------|------------------|
| 10/563,337 | 01/03/2006 | Siegried Koeppen | 20811/0204741-US0 | 8841 |
| 7278 | 7590 | 02/03/2010 | EXAMINER | |
| DARBY & DARBY P.C. P.O. BOX 770 Church Street Station New York, NY 10008-0770 | | | SU, SARAH | |
| | | | ART UNIT | PAPER NUMBER |
| | | | 2431 | |
| | | | MAIL DATE | DELIVERY MODE |
| | | | 02/03/2010 | PAPER |

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.



UNITED STATES PATENT AND TRADEMARK OFFICE

Commissioner for Patents
United States Patent and Trademark Office
P.O. Box 1450
Alexandria, VA 22313-1450
www.uspto.gov

**BEFORE THE BOARD OF PATENT APPEALS
AND INTERFERENCES**

Application Number: 10/563,337

Filing Date: January 03, 2006

Appellant(s): KOEPPEN ET AL.

Erik R. Swanson
Reg. No. 40,833
For Appellant

EXAMINER'S ANSWER

This is in response to the appeal brief filed 5 November 2009 appealing from the Office action mailed 18 February 2009.

(1) Real Party in Interest

A statement identifying by name the real party in interest is contained in the brief.

(2) Related Appeals and Interferences

The examiner is not aware of any related appeals, interferences, or judicial proceedings which will directly affect or be directly affected by or have a bearing on the Board's decision in the pending appeal.

(3) Status of Claims

The statement of the status of claims contained in the brief is correct.

(4) Status of Amendments After Final

The appellant's statement of the status of amendments after final rejection contained in the brief is correct.

(5) Summary of Claimed Subject Matter

The summary of claimed subject matter contained in the brief is correct.

(6) Grounds of Rejection to be Reviewed on Appeal

The appellant's statement of the grounds of rejection to be reviewed on appeal is correct.

(7) Claims Appendix

The copy of the appealed claims contained in the Appendix to the brief is correct.

(8) Evidence Relied Upon

| | | |
|-----------------|----------------|--------|
| 2004/0054750 A1 | de Jong et al. | 3-2004 |
| 2003/0174842 A1 | Challener | 9-2003 |
| 5,901,227 | Perlman | 5-1999 |
| 2004/0010715 A1 | Winiger et al. | 1-2004 |

(9) Grounds of Rejection

The following ground(s) of rejection are applicable to the appealed claims:

Claim Rejections - 35 USC § 103

1. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

(a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negated by the manner in which the invention was made.

2. Claims 2-10 and 13 are rejected under 35 U.S.C. 103(a) as being unpatentable over de Jong et al. (US 2004/0054750 A1 and de Jong hereinafter) and in view of Challener (US 2003/0174842 A1).

As to claim 2, de Jong discloses a system and method for digital content access control, the system and method having:

accessing the server over an internet (0081, lines 16-17);
sending, by the server (i.e. provisioner), **a client program** (i.e. tokens) **to a first local computer of the first user, the client program enabling an authentication of the first user using the user certificate and a transmission of at least one further security requirement** (0127, lines 1-3, 5-10);
setting up a personal main folder (i.e. content repository) **on the server for the first user, the main folder having a first special file** (i.e. content rights database) **including a first security requirement defined for the main folder and first management information so as to provide a main locker** (0098, lines 4-9; 0099, lines 4-7);
configuring the personal main folder to have at least one further folder (i.e. content associated with request) **set up therein, the at least one further folder having a function and a second file including a second security requirement** (i.e. token) **defined for the at least one further folder and including second management information so as to provide a functional locker** (0098, lines 9-14; 0099, lines 4-13, 16-19);
displaying the functional locker only if at least one security-relevant requirement is met so as to provide a locker system having a virtual character, wherein the functional locker provides (0102, lines 25-32):

a personal locker, wherein a reference to first files of the first user is storable in the personal locker only by the first user and displayable only to the first user, and at least one of;

a provisioning locker, wherein a first reference (i.e. URL) to a different second file for another user being storable by the first user (i.e. content producer) therein (0109, lines 2-3; 0110, lines 1-6; 0175, lines 1-4);

a receiving locker, wherein a third file of a sender user of the users is storable therein only by the second user, the receiving locker being configured, when opened, to provide to the first user a sender user reference relating to the storage of the third file and to a sender user defined security requirement.

De Jong fails to specifically disclose:

upon request, issuing, by an operator of the server, to a first user of the users a user certificate for access conditions, and providing the user certificate and a secret key to the first user.

Nonetheless, this feature is well known in the art and would have been an obvious modification of the teachings disclosed by de Jong, as taught by Challener.

Challener discloses a system and method for managing private keys, the system and method having:

issuing, upon request by an operator of the server (i.e. CA), to a first user of the users a user certificate for access conditions (0005, lines 1-7);

providing the user certificate and a secret key to the first user (0005, lines 1-7).

Given the teaching of Challener, a person having ordinary skill in the art at the time of the invention would have readily recognized the desirability and advantages of modifying the teachings of de Jong with the teachings of Challener by providing a user with a certificate and key. Challener recites motivation by disclosing that using encryption is a well known method of providing security for communications between two computers in a network (0004, lines 7-8). It is obvious that the teachings of Challener would have improved the teachings of de Jong by providing for encryption in order to secure communications.

As to claim 3, de Jong fails to specifically disclose:

wherein the certificate includes a public key.

Nonetheless, this feature is well known in the art and would have been an obvious modification of the teachings disclosed by de Jong, as taught by Challener.

Challener discloses:

wherein the certificate includes a public key (0005, lines 1-3).

Given the teaching of Challener, a person having ordinary skill in the art at the time of the invention would have readily recognized the desirability and advantages of modifying the teachings of de Jong with the teachings of Challener by using a public key in a certificate. Challener recites motivation by disclosing that using a public key in a certificate allows all parties to access the public key (0005, lines 5-6). It is obvious that

Art Unit: 2431

the teachings of Challener would have improved the teachings of de Jong by using a certificate with a key in order to allow all parties to have access to the key.

As to claim 4, de Jong fails to specifically disclose:

providing a public key to the first user.

Nonetheless, this feature is well known in the art and would have been an obvious modification of the teachings disclosed by de Jong, as taught by Challener.

Challener discloses:

providing a public key to the first user (0005, lines 4-6).

Given the teaching of Challener, a person having ordinary skill in the art at the time of the invention would have readily recognized the desirability and advantages of modifying the teachings of de Jong with the teachings of Challener by providing a public key to a user. Please refer to the motivation recited above in respect to claim 2 as to why it is obvious to apply the teachings of Challener to the teachings of de Jong.

As to claim 5, de Jong fails to specifically disclose:

wherein the providing the user certificate and the secret key to the first user is performed by providing the user certificate and the secret key on a smart card.

Nonetheless, this feature is well known in the art and would have been an obvious modification of the teachings disclosed by de Jong, as taught by Challener.

Challener discloses:

wherein the providing the user certificate and the secret key to the first user is performed by providing the user certificate and the secret key on a smart card (0008, lines 1-3).

Given the teaching of Challener, a person having ordinary skill in the art at the time of the invention would have readily recognized the desirability and advantages of modifying the teachings of de Jong with the teachings of Challener by providing key information on a smart card. Challener recites motivation by disclosing that smart cards are small and can hold memory and logic (0008, lines 1-2). It is obvious that the teachings of Challener would have improved the teachings of de Jong by providing key information on a smart card in order to provide security using a small device.

As to claim 6, de Jong discloses:

wherein the at least one further security requirement includes at least one of a biometric system requirement, a geographic positioning requirement, a time restriction, a network requirement, and a computer data requirement (0098, lines 19-22).

As to claim 7, de Jong discloses:

wherein the at least one further security requirement includes a time dependency (0164, lines 2-5).

As to claim 8, de Jong discloses:

wherein the at least one further security requirement is a requirement of at least one of the operator of the server, the first user, and the sender (i.e. user of one or more users) of the third file (0098, lines 4-8, 19-22).

As to claim 9, de Jong discloses:

wherein the provisioning locker has a name associated therewith (0110, lines 1-6).

As to claim 10, de Jong discloses:

wherein the provisioning locker includes a user locker for the another user (Abstract, lines 9-10).

As to claim 13, de Jong discloses:

wherein the first user and the second user are each registered with the server, and further comprising setting up a second personal main folder on the server for the second user registered with the server, the second main folder having a respective first special file including a respective first security requirement defined for the respective main folder and respective management information so as to provide a respective locker (0098, lines 4-9; 0099, lines 4-7),

configuring each respective main folder to have respective further folders set up therein, the respective further folders each having a respective function and each having a respective second file including a respective second security requirement defined for the respective further folders and including the respective management information, each of the further folders acting as a respective functional locker (0098, lines 9-14; 0099, lines 4-13, 16-19),

displaying each functional locker only if a respective security-relevant requirement is met, so as to provide a respective locker system having a virtual character (0102, lines 25-32), each functional locker providing a respective function of at least one of:

a respective personal locker, respective first files being storable in the respective personal locker only by the respective user and displayable only to the respective user;

a respective provisioning locker, wherein a respective first reference to a respective second file for a different user being storable by the respective user therein (0109, lines 2-3; 0110, lines 1-6; 0175, lines 1-4);

a respective receiving locker for a respective third file available to a respective sender user of the users, the respective receiving locker being configured, when opened, to provide to the respective user a respective sender user reference relating to the storage of the respective third file and to a respective sender user defined security requirement;

a respective public locker configured to store, by the first user, the first reference to the second file when the first reference is stored in the provisioning locker, if access to the first reference is offered to a plurality of different users.

The examiner notes that the process of claim 13 uses the similar process of claim 2 to create a second instance. It would have been obvious to one of ordinary skill in the art at the time the invention was made to repeat the same process of claim 2 to create another instance of the folder because a mere duplication only involves routine skill in the art.

3. Claims 14-16 are rejected under 35 U.S.C. 103(a) as being unpatentable over de Jong in view of Challener as applied to claim 2 above, and further in view of Perlman (US Patent 5,901,227).

As to claim 14, de Jong in view of Challener discloses:

**encrypting the data using the access key (0004, lines 8-10);
encrypting, by the server, the transmitted encrypted data a second time (0032, lines 5-8; 0033, lines 8-10).**

Given the teaching of Challener, a person having ordinary skill in the art at the time of the invention would have readily recognized the desirability and advantages of modifying the teachings of de Jong with the teachings of Challener by encrypting data with a key. Please refer to the motivation recited above in respect to claim 2 as to why it is obvious to apply the teachings of Challener to the teachings of de Jong.

De Jong in view of Challener fails to specifically disclose:

storing a fourth file in the functional locker only if the second security requirement is met;

generating a random number from data of the fourth file so as to provide an access key;

subsequently encrypting the access key with the public key and then destroying the access key so that the access key, for accessing the stored file, can only be recovered using the secret key;

receiving, at the server, the encrypted data, fourth management information of the fourth file, and the encrypted access key;

generating a unique file identifier for the fourth file;

storing the fourth file in a system locker using the file identifier;

storing a fourth reference to the fourth file in the functional locker, the fourth reference including the unique file identifier, the encrypted access key, and the fourth management information.

Nonetheless, these features are well known in the art and would have been an obvious modification of the teachings disclosed by de Jong in view of Challener, as taught by Perlman.

Perlman discloses a system and method for implementing partial and complete optional key escrow, the system and method having:

storing a fourth file in the functional locker only if the second security requirement (i.e. minimum fulfilled) is met (col. 5, lines 55-57; col. 6, lines 10-14);

generating a random number (i.e. nonce) from data of the fourth file so as to provide an access key (col. 1, lines 29-30). It would have been obvious to one of ordinary skill in the art at the time the invention was made to derive a random number from data since it is known in the art that linking data content to encryption increases security.

subsequently encrypting the access key with the public key and then destroying the access key so that the access key, for accessing the stored file, can only be recovered using the secret key (col. 4, lines 44-45, 47-49);

receiving, at the server, the encrypted data, fourth management information of the fourth file, and the encrypted access key (col. 5, lines 29-36);

generating a unique file identifier (i.e. UID) for the fourth file (i.e. escrow information) (col. 6, lines 46-48);

storing the fourth file in a system locker using the file identifier (col. 5, lines 55-57; col. 6, lines 32-33);

storing a fourth reference to the fourth file in the functional locker, the fourth reference including the unique file identifier, the encrypted access key, and the fourth management information (col. 5, lines 31-36).

Given the teaching of Perlman, a person having ordinary skill in the art at the time of the invention would have readily recognized the desirability and advantages of modifying the teachings of de Jong in view of Challener with the teachings of Perlman by transferring a hidden key and storing information. Perlman recites motivation by disclosing that encrypting keys ensures that the information is safe from an eavesdropper (col. 1, lines 43-45) and storing information using a pointer so that the information can be shared (col. 6, lines 19-22). It is obvious that the teachings of Perlman would have improved the teachings of de Jong in view of Challener by transferring a hidden key and storing information so that the information can be protected while being shared.

As to claim 15, de Jong in view of Challener discloses:

wherein the functional locker is the provisioning locker including a user file (i.e. messages) for the other user (0024, lines 5-7), and further including the steps of: enabling the stored fourth file to be forwarded by the first user to the other user only if the first user decrypts the encrypted access key with the secret key and re-encrypts the decrypted access key with a second public key of the other user (0033, lines 4-10), storing the re-encrypted access key, the file unique identifier and the fourth management information, as the fourth reference to the file into the user locker (0027, lines 11-14; 0033, lines 10-12).

Given the teaching of Challener, a person having ordinary skill in the art at the time of the invention would have readily recognized the desirability and advantages of modifying the teachings of de Jong with the teachings of Challener by re-encrypting the key and storing it with information. Challener recites motivation by disclosing that encrypting the key assures an administrator that the information is sent only to an authorized client (0035, lines 10-12). It is obvious that the teachings of Challener would have improved the teachings of de Jong by storing a re-encrypted key in order to ensure the integrity of the key.

As to claim 16, de Jong in view of Challener fails to specifically disclose:

wherein the second management information includes a management requirement, and wherein the storing the fourth file is performed only if the management requirement is met.

Nonetheless, this feature is well known in the art and would have been an obvious modification of the teachings disclosed by de Jong in view of Challener, as taught by Perlman.

Perlman discloses:

wherein the second management information includes a management requirement, and wherein the storing the fourth file (i.e. escrow information) is performed only if the management requirement is met
(col. 5, lines 55-57; col. 6, lines 10-14).

Given the teaching of Perlman, a person having ordinary skill in the art at the time of the invention would have readily recognized the desirability and advantages of modifying the teachings of de Jong in view of Challener with the teachings of Perlman by storing information only if a requirement is met. Perlman recites motivation by disclosing that only information that follows certain requirements, such as the requirements of a government (col. 6, lines 13-14) can be used. It is obvious that the teachings of Perlman would have improved the teachings of de Jong in view of Challener by storing information if a condition is met in order to ensure compliance with regulations.

4. Claims 11-12 are rejected under 35 U.S.C. 103(a) as being unpatentable over de Jong in view of Challener as applied to claim 2 above, and further in view of Winiger et al. (US 2004/0010715 A1 and Winiger hereinafter).

As to claim 11, de Jong in view of Challener fails to specifically disclose:

wherein the receiving locker has a name associated with a sender of the third file.

Nonetheless, this feature is well known in the art and would have been an obvious modification of the teachings disclosed by de Jong in view of Challener, as taught by Winiger.

Winiger discloses a system and method for specifying a repository for an authentication token, the system and method having:

wherein the receiving locker has a name associated with a sender (i.e. user) of the third file (i.e. password) (0039, lines 7-8).

Given the teaching of Winiger, a person having ordinary skill in the art at the time of the invention would have readily recognized the desirability and advantages of modifying the teachings of de Jong in view of Challener with the teachings of Winiger by using a name associated with data. Winiger recites motivation by disclosing that the use of identification information such as a name enables a system to perform operations such as a password change (0039, lines 3-7). It is obvious that the teachings of Winiger would have improved the teachings of de Jong in view of Challener by associating a name with data in order to provide for operations such as password changes.

As to claim 12, de Jong in view of Challener fails to specifically disclose:

wherein the receiving locker includes a user locker for the sender user.

Nonetheless, this feature is well known in the art and would have been an obvious modification of the teachings disclosed by de Jong in view of Challener, as taught by Winiger.

Winiger discloses:

wherein the receiving locker includes a user locker (i.e. storage of password in repository) for the sender user (0030, lines 3-4).

Given the teaching of Winiger, a person having ordinary skill in the art at the time of the invention would have readily recognized the desirability and advantages of modifying the teachings of de Jong in view of Challener with the teachings of Winiger by providing for a locker for a user. Winiger recites motivation by disclosing that storing a token with

which to compare inputted information allows for authentication (0004, lines 7-13). It is obvious that the teachings of Winiger would have improved the teachings of de Jong in view of Challener by providing a locker for a user in which to store data so that the information can be used for authentication.

(10) Response to Argument

Claims 2-10 and 13

It is argued by the Appellant that the teachings of de Jong fail to disclose of a *personal locker that contains references to files of a first user that are displayable only to that first user*. The Appellant further argues that the user of de Jong stores no reference to the file of the user and that de Jong does not disclose that the content storers is the only user to which a reference to the content is displayable.

The examiner respectfully disagrees with the Appellant's assertion. De Jong discloses that a content producer provides digital content to at least one content repository and a description of the content to at least one content provisioner (i.e. personal locker) (0175, lines 1-8) and that the description of the digital content may comprise a URL, part of a URL, a summary of the digital content, a hash of the digital content, or the like (0183, lines 5-7). Therefore, since the description of the digital content has been described as a link for the content, the description has been interpreted by the examiner as a reference to the content. Further, de Jong discloses that a token specifies a single digital content item made accessible by the token such that a presenting token entitles the presenter access to digital content (0114, lines 9-

13). A download manager in the provisioner verifies whether the user is authorized to access the digital content associated with the URL and receives the token if authorized (0184, lines 8-19). Since the content producer originally had access to the digital content by initially providing the content, the producer is authorized to access the digital content. De Jong also discloses that an indication is made when a token is redeemed so that a token is redeemed a predetermined number of times, where this predetermined number of times is one (0162, lines 9-13), thus making the digital content only available to the one user.

Claims 14-16

It is argued by the Appellant that Perlman neither teaches nor suggests the features of claims 14-16 demonstrated to be missing from de Jong and Challener of claim 2 above.

The examiner respectfully disagrees with the Appellant's assertion. As discussed above, de Jong discloses that a content producer provides digital content to at least one content repository and a description of the content to at least one content provisioner (i.e. personal locker) (0175, lines 1-8) and that the description of the digital content may comprise a URL, part of a URL, a summary of the digital content, a hash of the digital content, or the like (0183, lines 5-7). Therefore, since the description of the digital content has been described as a link for the content, the description has been interpreted by the examiner as a reference to the content. Further, de Jong discloses that a token specifies a single digital content item made accessible by the token such

that a presenting token entitles the presenter access to digital content (0114, lines 9-13). A download manager in the provisioner verifies whether the user is authorized to access the digital content associated with the URL and receives the token if authorized (0184, lines 8-19). Since the content producer originally had access to the digital content by initially providing the content, the producer is authorized to access the digital content. De Jong also discloses that an indication is made when a token is redeemed so that a token is redeemed a predetermined number of times, where this predetermined number of times is one (0162, lines 9-13), thus making the digital content only available to the one user.

In response to applicant's arguments against the references individually, one cannot show nonobviousness by attacking references individually where the rejections are based on combinations of references. See *In re Keller*, 642 F.2d 413, 208 USPQ 871 (CCPA 1981); *In re Merck & Co.*, 800 F.2d 1091, 231 USPQ 375 (Fed. Cir. 1986). It is noted that it is the teachings of de Jong that are relied upon for the claim limitations which have been argued.

Claims 11-12

It is argued by the Appellant that Winiger neither teaches nor suggests the features of claims 11-12 demonstrated to be missing from de Jong and Challener of claim 2 above.

The examiner respectfully disagrees with the Appellant's assertion. As discussed above, de Jong discloses that a content producer provides digital content to

at least one content repository and a description of the content to at least one content provisioner (i.e. personal locker) (0175, lines 1-8) and that the description of the digital content may comprise a URL, part of a URL, a summary of the digital content, a hash of the digital content, or the like (0183, lines 5-7). Therefore, since the description of the digital content has been described as a link for the content, the description has been interpreted by the examiner as a reference to the content. Further, de Jong discloses that a token specifies a single digital content item made accessible by the token such that a presenting token entitles the presenter access to digital content (0114, lines 9-13). A download manager in the provisioner verifies whether the user is authorized to access the digital content associated with the URL and receives the token if authorized (0184, lines 8-19). Since the content producer originally had access to the digital content by initially providing the content, the producer is authorized to access the digital content. De Jong also discloses that an indication is made when a token is redeemed so that a token is redeemed a predetermined number of times, where this predetermined number of times is one (0162, lines 9-13), thus making the digital content only available to the one user.

In response to applicant's arguments against the references individually, one cannot show nonobviousness by attacking references individually where the rejections are based on combinations of references. See *In re Keller*, 642 F.2d 413, 208 USPQ 871 (CCPA 1981); *In re Merck & Co.*, 800 F.2d 1091, 231 USPQ 375 (Fed. Cir. 1986). It is noted that it is the teachings of de Jong that are relied upon for the claim limitations which have been argued.

(11) Related Proceeding(s) Appendix

No decision rendered by a court or the Board is identified by the examiner in the Related Appeals and Interferences section of this examiner's answer.

For the above reasons, it is believed that the rejections should be sustained.

Respectfully submitted,

/Sarah Su/

Examiner, Art Unit 2431

Conferees:

/Christopher A. Revak/

Primary Examiner, Art Unit 2431

/William R. Korzuch/

Supervisory Patent Examiner, Art Unit 2431